

REMARKS

Reconsideration of the application is respectfully requested.

The claim amendments here are supported in the Specification as filed, and accordingly no new matter has been added. See, for example, Fig. 2 which clarifies the role of an application program in performing the different operations that are claimed. With claims 7-9, 16-18, 25-28, and 30 being canceled, the claims pending upon entry of this amendment are 1-6, 10-15, 19-24, and 29.

Addressing now the rejections in the order that they appear in the Office Action, claims 1-6, 10-15, 19-24, and 28-30 stand rejected as being anticipated by U.S. Patent No. 6,263,348 issued to Kathrow, et al. ("Kathrow"). According to the Office Action, beginning at page 3, in a Microsoft operating system, there is a process of authentication and generation of a hash value of a user password. The user enters her password and a client program hashes the password and sends a response to the server. In addition, in Kathrow, a method for determining that two files are different is described, by comparing hashed functions of them (instead of their contents explicitly). This yields a faster comparison when repeating the operation for a large number of files, e.g. Windows registry files in individual machines on a network. A portion of one file may be used to restore portions of another, corrupted file. The above, according to the Office Action, anticipates Applicants' claim 1.

To obviate the above rejection, claim 1 has been amended to clarify the claimed method for detecting tampering with registry settings in a computer. An application program running in the computer generates a user identity value associated with a user identity that is authorized to change a system registry of the computer. The application program also generates a registry security value associated with the system registry. The system registry is authenticated by the application program after reading the system registry. Kathrow does not teach or suggest such a method.

In Kathrow, the method for determining that two files are different is not taught or suggested as being performed by the same application program that also generates a user identity value. Separately, any teachings of the Microsoft NT operating system

(as described at the bottom of page 3 of the Office Action) refer to a client-server authentication procedure for allowing a client user access to a server process. This does not teach or suggest Applicants' claim 1 as amended here, which is designed to detect tampering with the registry settings in a computer, using an application program that is running in the computer to perform the recited operations. Accordingly, not only is claim 1 not anticipated by Kathrow, but it also would not have been obvious in view of Kathrow and the Microsoft NT operating system features recited in the Office Action at pages 3 and 4.

Turning now to claim 10, this claim has also been amended to obviate the anticipation rejection in view of Kathrow, by clarifying the combination of user identity authentication and system registry authentication. In particular, the claim refers to the capability of generating a user identity value associated with a user identity that is authorized to access a system registry of the machine. The user identity value is stored. A registry security value associated with the system registry is also generated and stored. A new user identity value associated with a new user identity that is seeking access to the system registry is generated. This new value is compared to the stored user identity value. The system registry is authenticated after being read. A one-way function is applied to the system registry settings as they are changed by the new user identity, to obtain a new registry security value, which is stored for a subsequent authentication of the system registry. Kathrow including the Microsoft NT operating system features described at pages 3 and 4 of the Office Action, do not anticipate nor do they render obvious such capability.

The process of authenticating a user in the Microsoft NT operating system, as described at pages 3 and 4 of the Office Action, refers to the interaction between a client and a server, and, in particular, a user of the client seeking access to a server process. In contrast, Kathrow is focusing on identifying the existence of differences between two files (albeit Windows registry files) by comparing their hash values rather than their explicit content. The motivation there is to save time, by performing the hash value comparison for a large number of networked machines (instead of making comparisons of the individual registry files of the machines). See Kathrow, col. 2, lines 12-26, which states: "Although the Windows registry file is relatively small, in a

company with tens of thousands of computers each containing a Windows registry, storing a copy of all of the Windows registries used by the employees of the company can utilize significant storage resources. Additionally, such a visual comparison is time-consuming and subject to error. Therefore, a system and method are needed which can quickly and easily determine whether a file, such as the Windows registry, is different from another file, such as a previously-stored version of the Windows registry . . .”

There would be no teaching or suggestion to one of ordinary skill in the art to combine the file checking technique described in Kathrow with the Microsoft NT operating system feature of authenticating a user of a server process (using the client to hash a password entered by the user and then send the hash value to the server).

Accordingly, claim 10 as amended here, is neither anticipated nor obvious in view of Kathrow.

Turning now to claim 19, this claim has been amended to obviate any art rejection in view of Kathrow, by reciting an apparatus having a data storage device that stores instructions which implement an application program, where the instructions, when executed by a processor of the apparatus, cause the processor to generate a user identity value associated with a user identity that is authorized to change a system registry of the apparatus, store the user identity value, and generate and store a registry security value associated with the system registry. The system registry is authenticated after reading, based on the stored registry security value. Although Kathrow in describing a method for determining the difference between two files suggests that two versions of a Windows registry file can be compared by hashing the files to produce fingerprints and comparing the fingerprints (rather than the explicit contents of the files), there is no teaching or suggestion to modify such a technique into an application program that not only generates and stores a registry security value and authenticates the system registry based on the stored registry security value, but also generates and stores a user identity value associated with a user identity who is authorized to change the system registry. The motivation in Kathrow is to save time by comparing the hash values of the Windows registries of a large number of network machines, not to detect tampering of a system registry using the capability recited in amended claim 19.

Turning now to claims 7-9, 16-18, and 25-27, these stand rejected as being anticipated by U.S. Patent No. 5,809,230 issued to Pereira ("Pereira"). The rejection is moot since those claims have been canceled.

Any dependent claims not mentioned above are submitted as being neither anticipated or obvious, for at least the same reasons given above in support of their respective base claims.

CONCLUSION

In sum, a good faith attempt has been made to address the rejections in the Office Action, leaving claims which are believed to be in condition for allowance.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP


Dated: January 9, 2006

By 
Farzad E. Arini, Reg. No. 42,261

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, Post Office Box 1450, Alexandria, Virginia 22313-1450 on January 9, 2006.


Margaux Rodriguez January 9, 2006